Министерство образования Кировской области

«Обеспечение безопасности персональных данных»

Докладчик:

Городилов Сергей Викторович

Руководитель направления ИБ, АСПЕКТ-СЕТИ

gors@aspectspb.ru

46-56-46, 30-13-23

Важные замечания!!!

- Ответственность за реализацию конкретных правовых и организационных мер на своей территории и в рамках своей организации несет её руководитель
- Представленные материалы являются результатом опыта работы докладчика в данной сфере, основанного на доступных на данный момент времени трактовках законодательства,
- Представленные формы, материалы и презентации не являются официальной позицией государства в сфере персональных данных
- Официальную трактовку тех или иных позиций законодательства и нормативных документов в области персональных данных осуществляют: Министерство связи и массовых коммуникаций РФ, Роскомнадзор РФ (только в рамках контроля и надзора), Суды РФ, а также ФСБ, ФСТЭК, Роструд и другие органы власти в рамках своей сферы компетенции.

Организационно-правовая часть

№	Дата проведения	Тема
1.	23.11.2017	Основы информационной безопасности. Персональные данные и другие категории конфиденциальной информации. Законодательство и нормативные документы в области защиты персональных данных
2.	14.12.2017	Правовые меры защиты персональных данных - КАДРЫ
3.	18.01.2018	Правовые меры защиты персональных данных – Образовательная деятельность

Организационно-техническая часть

4.	08.02.2018	Организационные меры защиты персональных данных
5.	01.03.2018	Информационные системы персональных данных (ИСПДн)
6.	15.03.2018	Модель угроз ПДн. Порядок защиты ИСПДн
7.	05.04.2018	Средства обеспечения ИБ в различных сценариях
8.	19.04.2018	Аттестация, сертификация и лицензирование в области защиты персональных данных. Контроль в области защиты персональных данных

Семинар №3

ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ - ФОРМЫ

Семинар №4

ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 18.1 пункт 1

- Оператор обязан принимать меры
- Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей

Статья 18.1 пункт 1

К таким мерам могут, в частности, относиться:

1) назначение ответственного за организацию обработки персональных данных;

2) издание оператором документов, определяющих:

- политику в отношении обработки персональных данных,
- локальных актов по вопросам обработки персональных данных, а также
- локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности ПДн;

Статья 18.1 пункт 1

4) осуществление внутреннего контроля и (или) аудита соответствия;

5) оценка вреда;

6) ознакомление работников оператора

- законодательства РФ о персональных данных,
- требованиями к защите ПДн,
- политикой оператора в отношении обработки ПДн,
- локальными актами по вопросам обработки ПДн,
- и (или) обучение указанных работников.

Политика ПДн

- 2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.
- Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Организационные меры

- Назначить
- Принятие процедур, инструкций, положений
- Работа с персоналом:
  - Доведение обязанностей, инструктажи, допуски, обязательства
  - Компетентность, квалификация
- Неавтоматизированная обработка ПДн
- Режимные меры
- Контроль обработки ПДн
- *Хорошие практики по организации обработки ПДн*

Основные нормативно-правовые документы:

- 152-ФЗ
- ПП РФ №687

Общие орг. документы

- приказ об организации обработки ПДн
- положение по организации обработки ПДн (включая форму типового согласия, журнала учета обращений, типового разъяснения)
- должностная инструкция лица, ответственного за организацию обработки ПДн
- приказ о перечне сотрудников, исполнение обязанностей которыми предполагает допуск к ПДн

Работа с персоналом

До

- Оценка компетентности и квалификации
- Составление и оценка досье
- Испытания

Во время

- Инструктажи
- Обязательства
- Обучение, тренинги, информирование
- Допуск к ценностям
- Квалифицирование

После

- Увольнение
- Перевод
- Возврат ценностей (материальных и нематериальных)

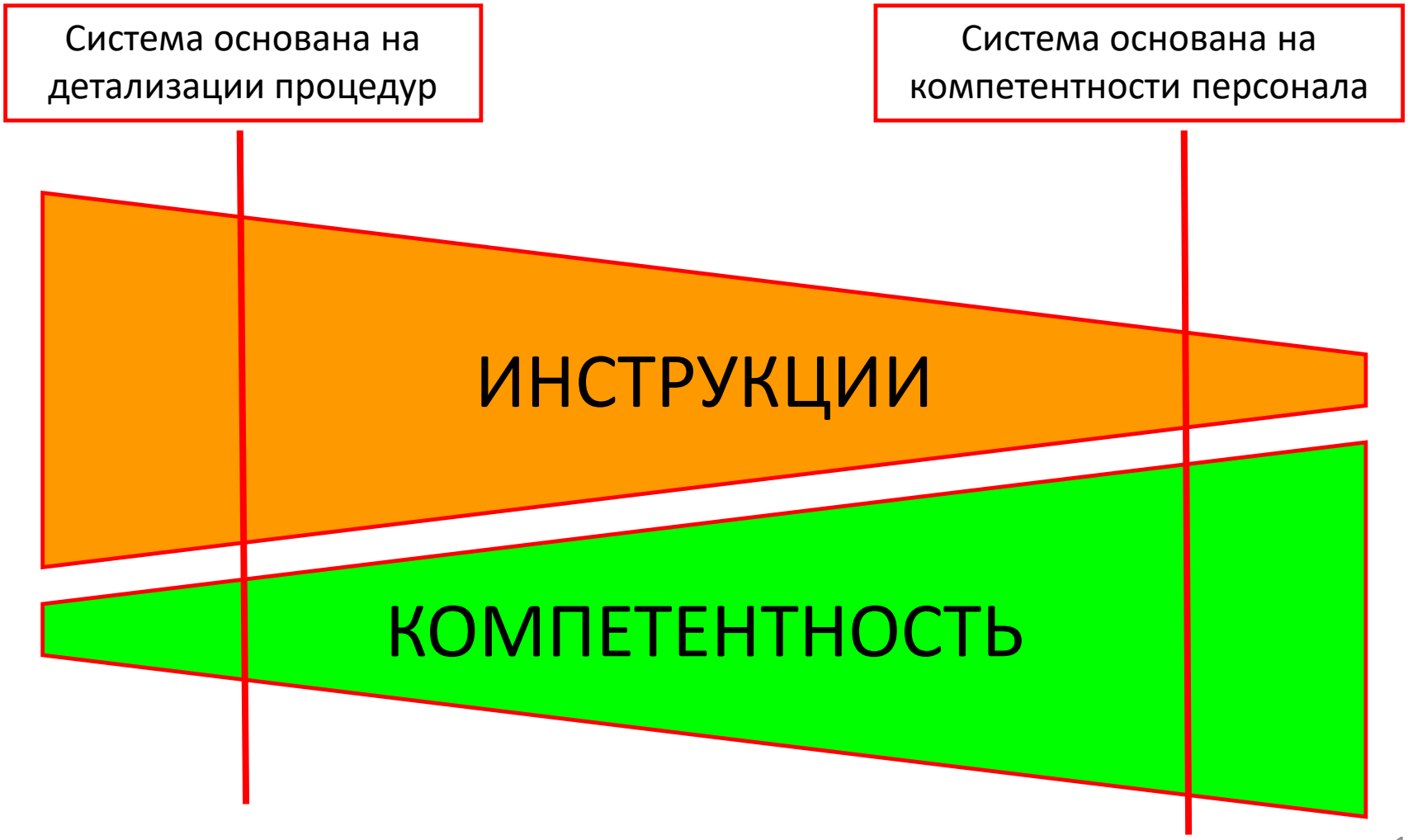
Компетентность

Ознакомление или компетентность?

Способы:

- Образование
- Обучение
- Тренинги
- Наставничество
- Информирование
- Опыт

Процедуры или доверие



Компетентность vs Квалификация

- Компетентность – образование, обучение, навыки и опыт.
- Квалификация – способность достигать результата. (От Qualify, квалифицирование)

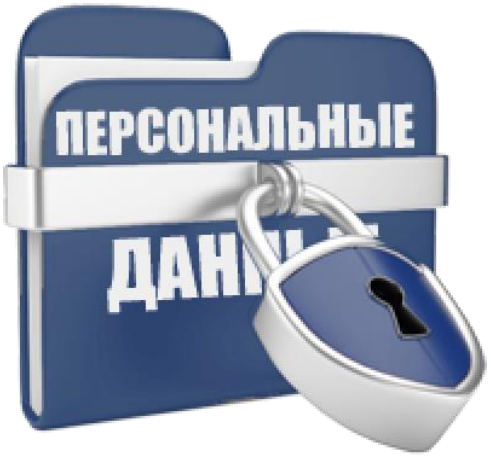
- В особо важных видах деятельности доверяют квалификации!

Неавтоматизированная обработка

Две ветви регулирования:

1. Согласно ПП РФ №687 – Документы с ПДн.

2. Согласно закону «Об архивном деле в Российской Федерации» №125-ФЗ - все документы.



или

Архивное дело

- Федеральный закон от 22 октября 2004 г. N 125-ФЗ «Об архивном деле в Российской Федерации»
- Уполномоченный орган - Министерство культуры Российской Федерации
- Перечень типов управленческих архивных документов, образующихся в процессе деятельности государственных органов , органов местного самоуправления, утверждённый приказом Министерства культуры Российской Федерации от 25.08.2010 № 558.

Согласно ПП РФ №687

Для всех документов с ПДн:

- Производится инвентаризация
  - документов
  - форм документов
- Утверждается перечень мест хранения:
  - Тип документа
  - Место хранения
  - Срок хранения
  - Ответственные лица
- **Может быть в номенклатуре дел!**

Формы документов

Для каждой формы должны быть определены:

- Порядок и цели сбора ПДн (в положении)
- Перечень полей
- Срок хранения
- Ответственные лица

Два варианта развития событий:

1. Форма утверждена вышестоящим ОГВ.
2. Форма собственная.

Пример формы Т-2 (Госкомстат РФ)

VII. НАГРАДЫ (ПООЩРЕНИЯ), ПОЧЕТНЫЕ ЗВАНИЯ

Наименование награды (поощрения)	Документ		
	наименование	номер	дата
1	2	3	4

VIII. ОТПУСК

Вид отпуска (ежегодный, учебный, без сохранения заработной платы и др.)	Период работы		Количество календарных дней отпуска	Дата		Основание
	с	по		начала	окончания	
1	2	3	4	5	6	7

IX. СОЦИАЛЬНЫЕ ЛЬГОТЫ, на которые работник имеет право в соответствии с законодательством

Наименование льготы	Документ		Основание
	номер	дата выдачи	
1	2	3	4

X. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

_____

_____

_____

_____

XI. ОСНОВАНИЕ ПРЕКРАЩЕНИЯ ТРУДОВОГО ДОГОВОРА (УВОЛЬНЕНИЯ) _____

Дата увольнения “ ” _____ 20 г.

Приказ (распоряжение) № _____ от “ ” _____ 20 г.

Работник кадровой службы _____ _____ _____
должность личная подпись расшифровка подписи

Работник _____
личная подпись

Унифицированная форма № Т-2
Утверждена постановлением Госкомстата РФ
от 5 января 2004 г. № 1

	Код
Форма по ОКУД	0301002
по ОКПО	

_____
наименование организации

Дата составления	Табельный номер	Идентификационный номер налогоплательщика	Номер страхового свидетельства государственного пенсионного страхования	Алфавит	Характер работы	Вид работы (основная, по совместительству)	Пол (мужской, женский)

ЛИЧНАЯ КАРТОЧКА работника

I. ОБЩИЕ СВЕДЕНИЯ

Трудовой договор	номер	
	дата	

1. Фамилия _____ Имя _____ Отчество _____

	Код
2. Дата рождения _____ (день, месяц, год)	
3. Место рождения _____ по ОКАТО	
4. Гражданство _____ по ОКИН	
5. Знание иностранного языка _____ (наименование) (степень знания) по ОКИН	
_____ по ОКИН	
6. Образование _____ (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное) по ОКИН	

Наименование образовательного учреждения	Документ об образовании, о квалификации или наличии специальных знаний			Год окончания
	наименование	серия	номер	
Квалификация по документу об образовании	Направление или специальность по документу			
	Код по ОКСО			

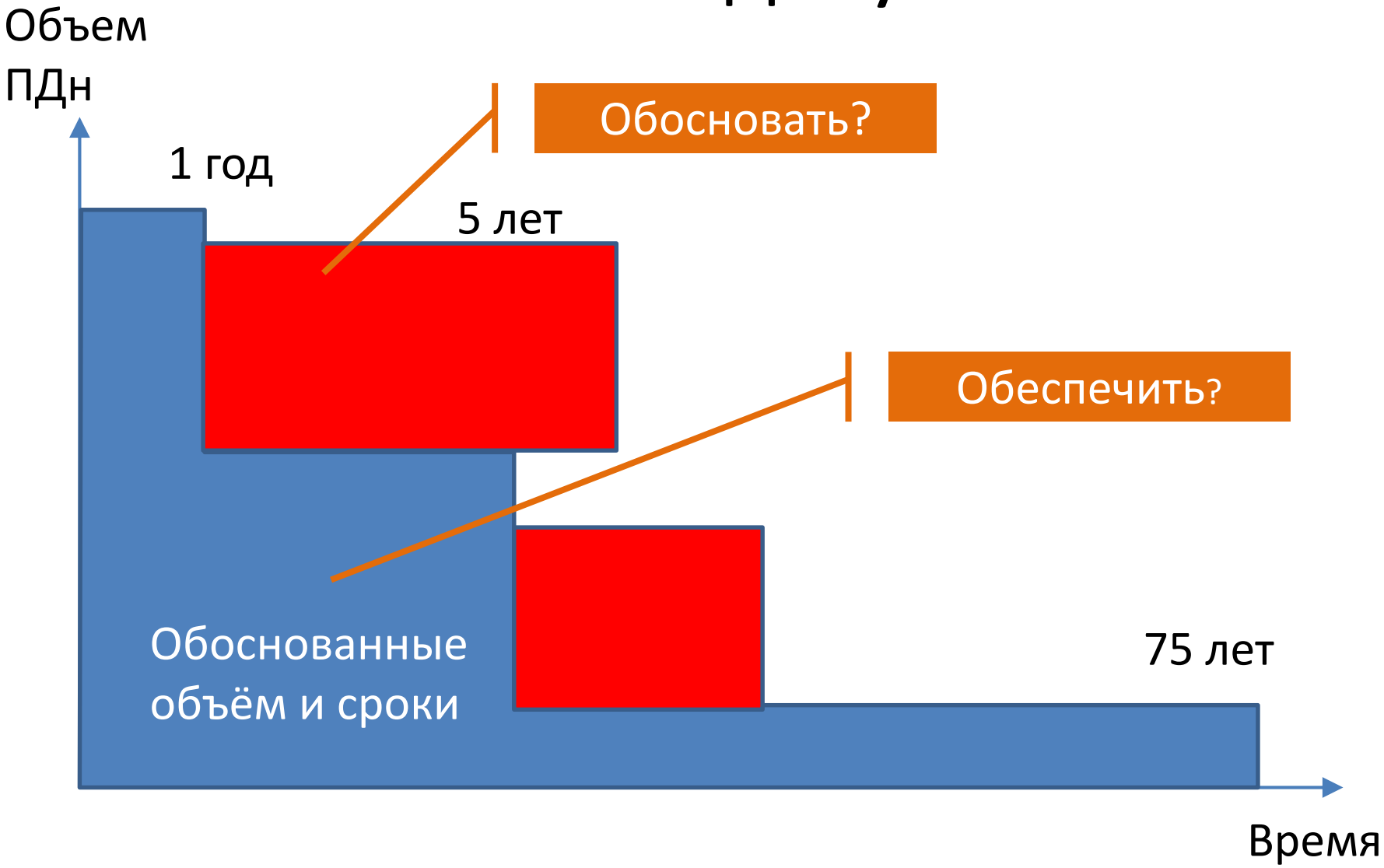
Наименование образовательного учреждения	Документ об образовании, о квалификации или наличии специальных знаний			Год окончания
	наименование	серия	номер	
Квалификация по документу об образовании	Направление или специальность по документу			
	Код по ОКСО			

Послевузовское профессиональное образование _____ Код по ОКИН
(аспирантура, адъюнктура, докторантура)

Наименование образовательного, научного учреждения	Документ об образовании, номер, дата выдачи	Год окончания
	Направление или специальность по документу	
	Код по ОКСО	

	Код
7. Профессия _____ (основная) по ОКПДТР	
_____ (другая) по ОКПДТР	

Уничтожение документов



Режимные меры

- Пропускной режим в здании
- Режим в помещениях
  - вход допущенных
  - посетители в присутствии допущенных
  - обслуживание
  - нештатные ситуации
- Учет ключей и ответственных
- Электронные системы безопасности
- Видеонаблюдение
- Охрана здания
- Обслуживание
- Нештатные ситуации

Контроль обработки ПДн

Акцент может быть на:

1. Квалификации ответственного
2. Составлении Акта-Протокола

Акт контроля

- Условия и основания обработки персональных данных;
- описание процессов обработки персональных данных;
- перечень персональных данных;
- перечень информационных систем персональных данных и их оценка;
- режимные мероприятия;
- организация обработки персональных данных;
- защита персональных данных;
- контроль объема и сроков обработки персональных данных как в автоматизированной форме, так и неавтоматизированной;
- заключение о соответствии и эффективности мероприятий;
- решения по улучшении системы организации обработки персональных данных.

Особые условия - ПДН

- Сферы ответственности (Режим, Неавт и ДО, ПДн, ИТ)
- Обратная связь
- Порядок допуска, ограничения доступа
- Прохождение документов
- Согласование условий обработки ПДн
- Контроль изменений условий работы
- Ознакомление

Ваши вопросы?

Спасибо за внимание!

Городилов Сергей

Руководитель направления ИБ, АСПЕКТ СПб

gors@aspectspb.ru

www.aspectspb.ru